

CASE NO.: ARC9-2000-0063-US1
Serial No.: 09/609,809
February 23, 2004
Page 10

PATENT
Filed: July 3, 2000

Remarks

Reconsideration of the above-captioned application is respectfully requested. Claims 1-7, 11, and 13 have been rejected under 35 U.S.C. §102 as being anticipated by Zhang, and the remaining claims have been rejected under 35 U.S.C. §103 as being obvious over Zhang in view of Enichen et al. Also, objections to the declaration, specification, drawings, and claims have been lodged.

Both now and at the time the present invention was made, both it and Enichen et al. were owned by and/or subject to an obligation to be assigned to the present assignee. Accordingly, Enichen et al. is removed as Section 103 prior art, leaving only the various objections and Section 102 rejection based on Zhang to be discussed.

To overcome the Examiner's claim objections, Claims 8, 12, and 14 have been amended as suggested, so the claim objections will not be further discussed. To overcome one of the objections to the specification, page 8 has been amended to recite diamond 32, not diamond 28, in the place indicated by the examiner. Claims 1-17 remain pending.

Objections to the Declaration

The declaration has been objected because it allegedly fails to provide a "post office address", citing Rule 33(a). Rule 33(a) requires a "correspondence address" be listed somewhere in the application, which it has been, e.g., above the inventor's signature on the declaration. The fact that the Office Action was correctly sent to this office is proof of that. Further, under the applicant's signature, a residence address appears, complete with zip code, so both a correspondence address and inventor's address have been provided as required.

1053-99.AMD

CASE NO.: ARC9-2000-0063-US1
Serial N.: 09/609,809
February 23, 2004
Page 11

PATENT
Filed: July 3, 2000

Objections to the Specification

In addition to the above-corrected objection, the examiner objects to pages 7 and 8 disclosing that "the result both changes...". There is nothing wrong with this. The referred-to result does two things: it both changes the ith block, and also becomes the new value B.

Objections to the Drawings

The drawings have been objected to for failing to show the second round of a DES cipher and for failing to show that odd-numbered rounds can be used in forward chaining and even-numbered in backward, as disclosed. However, Rule 83(a) requires drawings show each feature when such is necessary for an understanding of the invention. Here, disclosing what rounds of a cipher are used is sufficient in light of the logic shown in the drawings, without also showing a "round" of a cipher. Not every word in the disclosure must be "shown" in the drawings. Not surprisingly, the examiner fails to attempt to explain why the skilled artisan would not understand the invention if well-known cipher rounds are fully disclosed in the context of the drawings but are not "shown" in a box in a flow diagram.

Rejections Under 35 U.S.C. §102

Claims 1-7, 11, and 13 have been rejected under 35 U.S.C. §102 as being anticipated by Zhang, relying on col. 23, line 30 through col. 24, line 5. There are fundamental technical misunderstandings underpinning the rejection, rendering it improper. In summary, Zhang does not disclose block chaining at all, much less the manner in which it is presently claimed.

1053-99.AMD

CASE NO.: ARC9-2000-0063-US1
Serial No.: 09/609,809
February 23, 2004
Page 12

PATENT
Filed: July 3, 2000

Claims 1, 6, and 11 require plain text chaining, with Claims 1 and 11 specifically requiring forward and backward chaining. The only thing that Zhang does forward and backward is "scrambling"; evidently, the examiner considers Zhang's "scrambling" to be the equivalent of block chaining.

First, Zhang discloses "scrambling" the bits of a data block in both directions, not chaining adjacent blocks and then scrambling chained blocks prior to the next iteration in the chaining process in contrast to independent Claims 6, 11, and 13, all of which integrate the scrambling operation with the chaining operation. Specifically, in Zhang, the relied-upon col. 23 discloses only "scrambling" in a vacuum, using, specifically, either LZW compression as the scrambling function F^{-1} (col. 23, line 46) or DES encryption (line 47, which states that "*another example* [of the function F^{-1}] is the use of DES". As understood in the art, that indeed is what "scrambling" is: encryption, not block chaining, see MPEP §2111.01 (claims must be interpreted as those skilled in the art would interpret them). Furthermore, nowhere does Zhang teach doing something else within the "scrambling" iterations, whereas two things (block chaining, and scrambling) happen in independent Claims 6, 11, and 13 and in dependent Claim 3.

Thus, the conundrum faced by the examiner is simple. If Zhang's forward and backward "scrambling" is to be used as the present "chaining", what in Zhang correlates to the "scrambling" of Claims 6, 11, and 13? On the other hand, if Zhang's "scrambling" is used as the claimed scrambling, what in Zhang corresponds to the claimed block chaining?

Happily, both Zhang and the present application clear up the mystery. When Zhang uses the term "scrambling", not surprisingly it uses it in the same way as the present invention, namely, as a synonym for encryption. DES encryption, which Zhang discloses as an engine for the relied-upon forward and backward

1053-99.AM13

CASE NO.: ARC9-2000-0063-US1
Serial No.: 09/609,809
February 23, 2004
Page 13

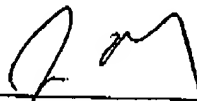
PATENT
Filed: July 3, 2000

operation - indeed scrambles, i.e., encrypts, data. That is the same way the present application uses the term, see, e.g., the discussion of block 30 on page 7 of the specification.

This lays bare the principal technical misunderstanding in the rejection, namely, that Zhang teaches block chaining. Nowhere does Zhang chain one block to another, much less does it institute scrambling within chaining iterations. Rather, the closest Zhang gets to the presently preferred XOR chaining function is in uncited column 22, line 48 continuing to col. 23, line 23, but Zhang does not use the XOR for the claimed block chaining. Rather, Zhang uses it on individual bytes within a block, and it does not do it "forward and backward" as required in Claim 1 and 11. So not only does Zhang fail to use an XOR (or anything else) to chain blocks as that phrase is understood in the art, it also fails to use it in a forward and backward process. As stated above, the only thing Zhang does "forward and backward" is scramble, which is not the same thing as chaining, much less block chaining.

The Examiner is cordially invited to telephone the undersigned at (619) 338-8075 for any reason which would advance the instant application to allowance.

Respectfully submitted,



John L. Rogitz
Registration No. 33,549
Attorney of Record
750 B Street, Suite 3120
San Diego, CA 92101
Telephone: (619) 338-8075

JLR:jg

1003-99.AMD